

DOD PRIVACY IMPACT ASSESSMENT (PIA)

1. DA organizational name (APMS Sub Organization name):

U.S. Army Corps of Engineers (USACE)

2. Name of Information Technology (IT) System (APMS System name):

Corps of Engineers Financial Management System (CEFMS)

3. Budget System Identification Number (SNAP-IT Initiative Number):

9997

4. System Identification Number(s) (IT Registry/Defense IT Portfolio Repository (DITPR/Army AITR):

2775

5. IT Investment (OMB Circular A11) Unique Identifier (if applicable)

202-00-01-01-01-1010-00

6. Privacy Act System of Records Notice Identifier (if applicable):

A0037-2-1 CE, Corps of Engineers Management Information System Files (February 22, 1993, 58 FR 10002)

T7332, Defense Debt Management System (June 27, 2002, 67 FR 43292)

7. OMB Information Collection Requirement Number (if applicable) and expiration date:

N/A

8. Type of Authority to collect information (statutory or otherwise):

Debt Collection Act of 1982 (Pub.L. 97-365, as amended by Pub.L. 104-134, the Debt Collection Improvement Act of 1996);

Pub.L. 89-508;

5 U.S.C. 301, Departmental Regulations

E.O. 9397 (SSN);

DoD 7000.14-R, Department of Defense Financial Management Regulation, Volume 5, Part 2

USACE Engineer Regulation 37-1-30, Financial Administration-Accounting and Reporting

9. Provide a brief summary or overview of the IT system:

CEFMS is the USACE corporate, web-based automated information system (AIS) for managing and transacting financial and accounting business processes. Financial transactions are entered directly into CEFMS for all appropriation accounting, administrative control of funds, time and attendance posting and labor distribution, accounts payable, accounts, accounts receivable, disbursing/collections, debt management, travel management, acquisition, asset management, inventory control, personnel/manpower, budget formation and execution and financial reporting. It is used to compute employee labor and travel costs charged to the job worked on in the management of financial expenditures and to administratively manage the collection of debts owed to the Department of Defense (DoD). These debts include, but are not limited to, overpayments, fines, interest, penalties, administrative fees, and amounts derived from damages, leases, and sales of real or personal property. CEFMS is used to implement the salary offset provisions of 5 U.S.C. 5514, the administrative offset provisions of 31 U.S.C. 3711 and 3716-3718, and the provisions of the Federal Claims Collection Standards (31 CFR parts 900-904), that apply to personal debts; to permit collection of delinquent claims and debts owed to the U.S. Government under any program or service administered by any creditor DoD Component; to determine the validity of waivers or to make referrals to the Defense Office of Hearings and Appeals (DOHA); to maintain records of investigations conducted for the purpose of confirming, canceling, or determining if the debts are accurate or valid, and whether the debt should be remitted or waived. CEFMS includes electronic signature creation and verification to ensure data integrity and internal control for all transactions leading to the disbursement of funds. This field-level financial management tool integrates USACE work management functions with accounting requirements prescribed under U.S. Government Standard General Ledger (USSGL) policies. CEFMS records all transactions, stores records electronically for easy access and retrieval, and updates USSGLs as each transaction is recorded. Although CEFMS is a single application, each District, Field Operating Activity (FOA), and Regional Business Center (RBC) within USACE has its own stand-alone instance of a CEFMS database. CEFMS integrates financial data with other Corps of Engineers automated systems and interfaces with other Department of Defense (DoD) systems.

10. Describe what information in identifiable form will be collected and the nature and source of the information:

CEFMS contains personally identifiable information on USACE personnel to include name, social security number (SSN), home address, bank account number, and Government issued credit card number to process payroll, record personnel costs, and manage the Government issued Credit Card Program. CEFMS contains some Privacy Act data on some DOD personnel to the extent needed to allow them access to the system and its records during audits. CEFMS also contains some Privacy Act data on other Federal personnel (non-USACE) to fill specific needs as requested by the other agency. CEFMS contains Privacy Act data on USACE contractors, including bank

account numbers and Tax Identification Numbers (TIN) to process payments and to report tax information to the Internal Revenue Service.

11. Describe how the information will be collected:

Non-government employees provide Tax Identification Number (TIN), bank account numbers, and address directly to USACE sites. This information is also obtained by queries of the DFAS Central Contractor Registration System (CCR). Data obtained from DFAS Central Contractor Registration System (CCR) is entered into CEFMS manually. USACE employees provide SSN to DOD personnel offices where data is maintained in the Defense Civilian Personnel Data System (DCPDS) and transferred to CEFMS biweekly. Government issued credit card numbers are entered by authorized data managers and are associated with individuals who have authority to use the card.

12. Describe the requirement and why the information in identifiable form is to be collected:

See #10 above.

13. Describe how the information in identifiable form will be used:

See #10 above.

14. Describe whether the system derives or creates new data about individuals through aggregation:

The system does not create new data about individuals through aggregation.

15. Describe with whom the information in identifiable form will be shared, both within DA and outside DA:

To the U.S. General Accounting Office, the U.S. Department of the Justice, Internal Revenue Service, U.S. Department of Treasury, or other Federal agencies for further collection action on any delinquent account when circumstances warrant. To any Federal agency where the debtor is employed or receiving some type of payment from that agency for the purpose of collecting debts owed the U.S. Government by non-centralized offset. Non-centralized offset encompasses an offset program administered by any Federal agency other than the U.S. Department of Treasury. The collection may be accomplished either voluntarily or involuntarily by initiating administrative or salary offset procedures under the provisions of the Debt Collection Act of 1982 (Pub.L. 97-365, as amended by Public Law. 104-134, the Debt Collection Improvement Act of 1996). To the U.S. Department of Treasury (DOT) for centralized administrative or salary offset, including the offset of Federal income tax refunds, for the purpose of collecting debts owed the U.S. Government; to the DOT contracted private collection agencies for the purpose of obtaining collection services, including administrative wage garnishment (AWG) in accordance with the Debt Collection Improvement Act of 1996

(Pub.L. 104-134), 31 U.S.C. 3720D, and 31 CFR Part 285, to recover monies owed to the U.S. Government. To the U.S. Department of Veteran Affairs for administration of laws pertaining to veterans' benefits. To any Federal agency for the purpose of accomplishing the administrative procedures to collect or dispose of a debt owed to the U.S. Government. This includes, but is not limited to, the Office of Personnel Management for personnel management functions and the Internal Revenue Service to obtain a mailing address of a taxpayer for the purpose of locating such taxpayer to collect or compromise a Federal claim against the taxpayer pursuant to 26 U.S.C. 1603(m)(2), and in accordance with 31 U.S.C. 3711, 3217, and 3718. The Internal Revenue Service may also request locator service for delinquent accounts receivable in order to report closed out accounts as taxable income, including amounts compromised or terminated, and accounts barred from litigation due to age. To any Federal, state, or local agency for the purpose of conducting an authorized computer-matching program to identify and locate delinquent debtors for recoupment of debts owed DoD. To publish or otherwise publicly disseminate information regarding the identity of the debtor and the existence of the non-tax debt, subject to review by the Secretary of the Treasury. The information will be shared only with individuals who have a need to know. The USACE participates along with all other federal agencies in the Treasury Offset Program System (TOPS) in an effort to collect debts due to all federal agencies. Through a central repository of debts administered by the U.S. Treasury, all federal agencies use for comparison the tax id number of debtors to identify outstanding debts owed to the federal government. If a match between a debtor and a federal agencies' pending payment is found, an offset is processed and amounts redirected to the U.S. Treasury in collection of the outstanding debt.

Internal DoD agencies that would obtain access to PII in this system, on request in support of an authorized investigation or audit, may include DOD IG, DCIS, Army Staff Principals in the chain of command, DAIG, AAA, USACIDC, INSCOM, PMG and ASA FM&C. In addition, the DoD blanket routine uses apply to this system.

16. Describe any opportunities individuals will have to object to the collection of information in identifiable form about themselves or to consent to the specific uses of the information in identifiable form:

Individuals are provided a Privacy Act advisory statement which indicates that furnishing information is voluntary. Failure to provide some information could mean that the employee or contractor will not be paid for their work, products or services.

17. Describe the process regarding how the individual is to grant consent:

Individuals are provided a Privacy Act advisory statement as information is being collected which indicates that furnishing information is voluntary.

18. Describe any information that is provided to an individual and the format of such information and means of delivery:

Individuals are provided a Privacy Act advisory in electronic and hardcopy format.

19. Describe the administrative/business, physical, and technical processes and controls adopted to secure, protect, and preserve the confidentiality of the information in identifiable form:

The data is stored within a secure datacenter on a secure Army Installation with all protections afforded by Army and Defense Information System Agency (DISA) security infrastructure. The datacenter has passed the required security measures tests required for Information Assurance System Accreditation and has a full Authority to Operate. Additionally, the system is built on redundancy with a full Continuity of Operations (COOP) site.

All aspects of privacy, security, configuration, operations, data retention and disposal in regards to information in identifiable form are documented in policies to ensure that privacy and security are consistently enforced and maintained. The impact of loss was evaluated for the information in identifiable form and is protected accordingly. A user's manual was designed to fulfill the needs of the different types of employees (e.g., users, administrators, managers, security officers) who will use the system. This system has a comprehensive security system that controls access to records. Access can be granted on an individual or group basis. The confidentiality of all data is protected by measures appropriate for unclassified system high operations with "need-to-know controls". All users are appropriately cleared for privileges based on individual user job requirements. Privileges are limited to only those necessary for job requirements.

20. Identify whether the IT system or collection of information will require a System of Records notice. If not published, state when publication of the notice will occur:

Existing Army SORNs apply (see #6 above).

21. Describe/evaluate any potential privacy risks the collection, use, and sharing of the information in identifiable form:

Due to the level of safeguarding, we believe the risk to individuals' privacy to be minimal. There are no risks in providing an individual the opportunity to object or consent, or in notifying individuals. Risk is mitigated by consolidation and linkage of files and systems, derivation of data, accelerated information processing and decision making, and use of new technologies.

22. Describe/evaluate any privacy risks in providing individuals an opportunity to object/consent or in notifying individuals:

None.

23. Describe/evaluate any risks posed by the adopted security measures:

None.

24. State classification of information/system and whether the PIA should be published or not. If not, provide rationale:

Data in the system is unclassified, for official use only.

25. If a PIA is planned for publication, state whether it will be published in full or summary form:

The PIA may be published in full.